



## CYBER ARK SECURE BROWSER

**DOCUMENT PURPOSE:** THIS TEMPLATE IS TO BE COMPLETED BY PARTNER AND IS REQUIRED FOR CYBERARK SECURED CERTIFICATION. THE AAM INTEGRATION TECHNICAL DOCUMENTATION WILL BE MADE AVAILABLE TO PARTNERS, CUSTOMERS AND PROSPECTS. **AS YOU COMPLETE EACH SECTION, PLEASE REMOVE THE DIRECTIONS PROVIDED.**

Name of Company: Votiro

Website: <https://votiro.com/>

Date: April 9, 2024

## INTEGRATION OVERVIEW

By combining the strengths of CyberArk Secure Browser and Votiro's Zero Trust Cloud, organizations can establish a robust, multi-layered defense that fortifies their cyber resilience and safeguards their digital assets. This integrated solution not only mitigates the risks associated with browser-based attacks but also neutralizes the threats posed by malicious file content, ensuring a safe and secure digital environment for employees and stakeholders.

## KEY BENEFITS

With CyberArk Secure Browser, organizations gain a secure and feature-rich browsing experience tailored for the enterprise. Its security-first design protects against web-based threats, enforces granular access controls to sensitive business applications, and provides visibility into user activity, while maintaining a seamless and productive user experience.

Complementing this, Votiro's Zero Trust Cloud employs advanced file sanitization techniques, leveraging patented Content Disarm and Reconstruction (CDR) technology to proactively prevent zero-day exploits, undisclosed attacks, and known threats from infiltrating the organization through files. This defense-in-depth solution offers real-time privacy and compliance monitoring, actionable data insights, and seamless integration with existing security infrastructure.

## CYBERARK SECURE BROWSER DOCUMENTATION AND INSTALLATION INSTRUCTIONS

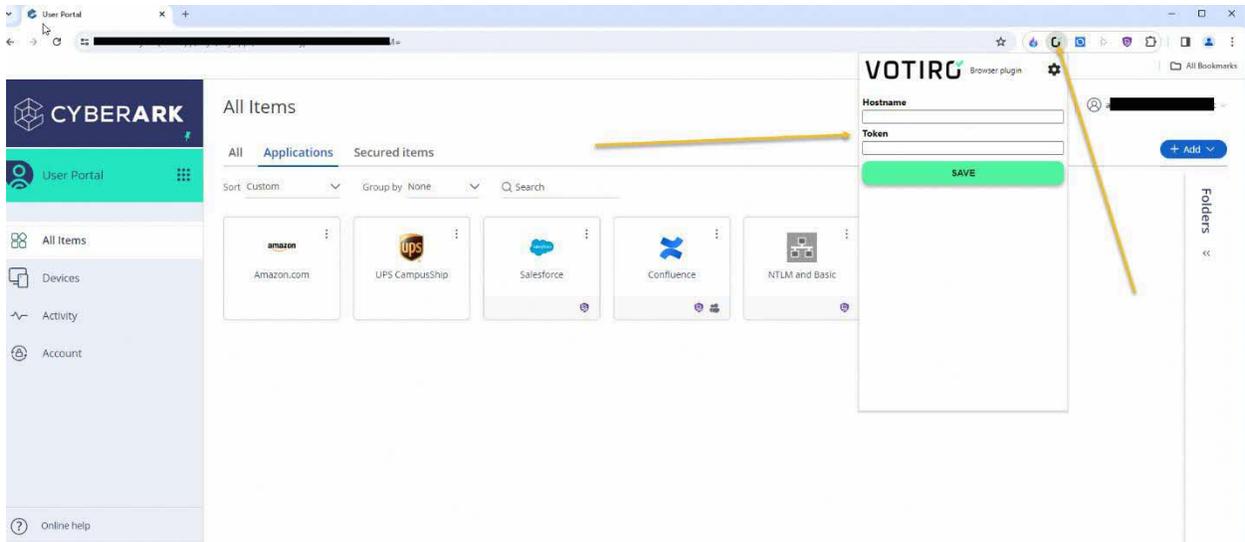
### [CSB Documentation](#)

### **Steps how to enable Votiro browser extension in Cyberark Secure Browser**

1. Open and authenticate to Cyberark Secure Browser
2. Navigate to Chrome store link [Votiro Browser plug-in](#) and select “Add to Chrome”.

Note: Make sure plug-in is not blocked by admin and if necessary, whitelist it.

3. Obtain from Votiro information which is required to establish connection with Votiro service that includes service token and host. Follow steps for generating [Service Token](#)



4. After the plugin is successfully installed and configured, you can test file downloads. You can see threat detection history by clicking Votiro's plugin. For more information on how to configure Votiro's policies or details about detected threats please refer to [Votiro support documentation](#)

